Net-Centric Implementation Framework

Part 1: Overview

Part 2: Traceability

Part 3: Migration Guidance

Part 4: Node Guidance

Part 5: Developer Guidance

Part 6: Contracting Guidance for Acquisition

V 2.2.0

17 June 2008

Net-Centric Enterprise Solutions for Interoperability (NESI) is a collaborative activity of the USN Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I); the USAF Electronic Systems Center (ESC); and the Defense Information Systems Agency (DISA).

Approved for public release; distribution is unlimited.

Table of Contents

Perspectives

P1117: NESI Executive Summary

Net-Centric Enterprise Solutions for Interoperability (**NESI**) provides, for all phases of the acquisition of net-centric solutions, actionable guidance that meets DoD Network-Centric Warfare goals. The guidance in NESI is derived from the higher level, more abstract concepts provided in various directives, policies and mandates such as the Net-Centric Operations and Warfare Reference Model (NCOW RM) [R1176] and the ASD(NII) Net-Centric Checklist [R1177] . As currently structured, NESI implementation covers architecture, design and implementation; compliance checklists; and a collaboration environment that includes a repository.

More specifically, NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for military application. NESI provides specific technical recommendations that a DoD organization can use as references. Stated another way, NESI serves as a reference set of compliant instantiations of these directives.

NESI is derived from a studied examination of enterprise-level needs and, more importantly, from the collective practical experience of recent and on-going program-level implementations. It is based on today's technologies and probable near-term technology developments. It describes the practical experience of system developers within the context of a minimal top-down technical framework. Most, if not all, of the guidance in NESI is in line with commercial best practices in the area of enterprise computing.

NESI applies to all phases of the acquisition process as defined in DoD Directive 5000.1 [R1164] and DoD Instruction 5000.2 [R1165] and to both new and legacy programs. NESI provides explicit counsel for building in net-centricity from the ground up and for migrating legacy systems to greater degrees of net-centricity.

NESI subsumes a number of references and directives; in particular, the Air Force C2 Enterprise Technical Reference Architecture (C2ERA) and the Navy Reusable Applications Integration and Development Standards (RAPIDS). Initial authority for NESI is per the Memorandum of Agreement between Commander, Space and Naval Warfare Systems Command (SPAWAR); Navy Program Executive Officer, C4I & Space (now PEO C4I); and the United States Air Force Electronic Systems Center (ESC), dated 22 December 2003, Subject: Cooperation Agreement for Net-Centric Solutions for Interoperability (NESI). The Defense Information Systems Agency (DISA) formally joined the NESI effort in 2006.

Content Structure

Perspectives	NESI **Perspectives** describe a topic and encompass related, more specific Perspectives or encapsulate a set of Guidance and Best Practice details, Examples, References, and Glossary entries that pertain to the topic.
Guidance	NESI **Guidance** is in the form of atomic, succinct, absolute and definitive Statements related to one or more Perspectives. Each Guidance Statement is linked to Guidance Details which provide Rationale, relationships with other Guidance or Best Practices, and Evaluation Criteria with one or more Tests, Procedures and Examples which facilitate validation of using the Guidance through observation, measurement or other means. Guidance Statements are intended to be binding in nature, especially if used as part of a Statement of Work (SOW) or performance specification.
Best Practices	NESI **Best Practices** are advisory in nature to assist program or project managers and personnel. Best Practice Details can have all the same parts as NESI Guidance. The use of

	NESI Best Practices are at the discretion of the program or project manager.
Examples	NESI *Examples* illustrate key aspects of Perspectives, Guidance, or Best Practices.
Glossary	NESI *Glossary* entries provide terms, acronyms, and definitions used in The context of NESI Perspectives, Guidance and Best Practices.
References	NESI *References* identify directives, instructions, books, Web sites, and other sources of information useful for planning or execution.

Releasability Statement

NESI *Net-Centric Implementation* v2.2 has been cleared for public release by competent authority in accordance with DoD Directive 5230.9 [R1232] and is granted Distribution Statement A: Approved for public release; distribution is unlimited. Obtain electronic copies of this document at http://nesipublic.spawar.navy.mil.

Vendor Neutrality

The NESI documentation sometimes refers to specific vendors and their products in the context of examples and lists. However, NESI is vendor-neutral. Mentioning a vendor or product is not intended as an endorsement, nor is a lack of mention intended as a lack of endorsement. Code examples typically use open-source products since NESI is built on the open-source philosophy. NESI accepts inputs from multiple sources so the examples tend to reflect whatever tools the contributor was using or knew best. However, the products described are not necessarily the best choice for every circumstance. Users are encouraged to analyze specific project requirements and choose tools accordingly. There is no need to obtain, or ask contractors to obtain, the tools that appear as examples in this guide. Similarly, any lists of products or vendors are intended only as references or starting points, and not as a list of recommended or mandated options.

Disclaimer

Every effort has been made to make NESI documentation as complete and accurate as possible. Even with frequent updates, this documentation may not always immediately reflect the latest technology or guidance. Also, references and links to external material are as accurate as possible; however, they are subject to change or may have additional access requirements such as Public Key Infrastructure (PKI) certificates, Common Access Card (CAC) for user identification, and user account registration.

Contributions and Comments

NESI is an open project that involves the entire development community. Anyone is welcome to contribute comments, corrections, or relevant knowledge to the guides via the Change Request tab on the NESI Public site, http://nesipublic.spawar.navy.mil, or via the following email address: nesi@spawar.navy.mil.

P1286: Part 1: Overview

Part 1: Overview is the first of six parts that comprise the NESI **Net-Centric Implementation** documentation set. Part 1 includes a high-level **Net-Centric Enterprise Solutions for Interoperability** general overview to provide awareness of NESI to a broad range of interested stakeholders.

NESI Purpose

NESI supports government and industry system and software engineers who are developing net-centric solutions as well as their associated program managers. Portions of NESI also pertain to contracting officers and end users.

The key value of NESI to program-level management and engineering personnel across the DoD is to make informed architectural and engineering decisions in support of achieving enterprise-level objectives related to Network-Centric Warfare. In general, these enterprise-level objectives relate to broad-scale data interoperability and overall system flexibility. While these objectives occasionally compete with program-level objectives of meeting specific cost, schedule, and performance goals, it is anticipated that achieving these enterprise-level objectives will result in an overall long-term benefit to the DoD.

More specifically, NESI attempts to provide acquisition programs a practical means for addressing DoD Network-Centric Warfare policy, directives, mandates, and other guidance documentation. NESI is not intended to replace existing policy, directives, and mandates, but rather helps to translate them into concrete actions for evaluation by program personnel. By considering the body of knowledge within NESI, an acquisition program is not guaranteed to be compliant with this direction, but program personnel should be better positioned to explain any deviation from it and consequently help programs pass Milestone reviews. By using NESI, program personnel and other stakeholders should have an increased level of confidence in the net-centricity of a specific program or set of programs.

NESI also lays the technical groundwork for developing an approach to assessing a program's degree of net-centricity within certain limitations. The most important contribution of NESI in this regard is to provide a framework for addressing specific topics that surround the often difficult trade-off decisions made among realizing various enterprise- and program-level objectives.

Goals

Key NESI goals include the following:

- Promote realization of the net-centric aspects of the GIG architecture, per the **DoD Global Information (GIG) Architecture** [R1170] , through the evolution of legacy systems and the development of new systems that comply with DoD net-centric direction.

- Promote the consistent application of a sound technical approach to net-centricity based on a component-based N-tier framework for application development. (Note: this framework may be implemented in many different ways; e.g., with different infrastructure distribution strategies).

- Promote the reuse of software components so that they can be composed easily into new mission capabilities with minimal development effort. NESI establishes a technical basis that allows developers to leverage reuse opportunities.

- Promote enterprise integration and interoperability through the reuse of enterprise design patterns, well-defined public service interfaces, and loosely coupled components. These are key elements to meet the criteria in the **Net-Centric Operations and Warfare Reference Model (NCOW RM)** [R1176] .

- Provide a model for the distribution of infrastructure elements in which Enterprise Services are provided and managed across the enterprise by the NCES program and individual programs share infrastructure resources in a Node-based approach.

Vision

The vision for NESI is that it will be the definitive source of net-centric implementation guidance for the DoD. The knowledge expressed in NESI will be accurate, current, accessible, cover all pertinent technical areas, and be easy to maintain. In addition, NESI will provide flexible tools for using this knowledge to achieve shared objectives across diverse organizations.

Development Strategy

To achieve the NESI vision, the developers of NESI will, in coordination with the rest of the acquisition, research, and user communities (to include government and industry representatives) do the following:

- Define related terms and concepts

- Identify specific architectural and engineering knowledge at multiple levels of abstraction:

  - Identify succinct, atomic, actionable guidance

  - Define the context for the guidance

  - Identify, define, and develop examples

  - Identify appropriate reference material

- Vet this knowledge across pertinent communities

- Identify tools to store, tag, sort, filter, and distribute this knowledge

- Maintain this knowledge

  - evolve as the concept of net-centricity evolves

  - remain current with changes in DoD net-centric directives, mandates, and instructions

Individual pieces of guidance will also be tagged with such metadata as source, currency (i.e., effective dates), and perceived importance (by organization). Individual pieces of guidance will also be capable of being tagged by using communities for specific uses such as indicating the scope of application for a particular piece of guidance. Individual pieces of guidance will also be capable of being grouped arbitrarily into potentially overlapping sets, called perspectives, that group common topics together (such as security or data) for ease of reference.

Development Governance

A governing body consisting of representatives from participating DoD organizations oversees the evolution of NESI. This body sets priorities for the execution of specific aspects of the NESI development strategy described above. This body meets on a regular basis to review NESI development plans and progress and to ensure adequate configuration management and content distribution mechanisms are in place.

Change Summary for v2.2

The primary focus of NESI v2.2 includes moving *Part 1: Overview* and *Part 2: Traceability* into NESI-X, the eXtensible Markup Language (XML) data base management system that the NESI team developed and maintains, deleting several unused Glossary items (i.e., linked to content which no longer is in the current version), and adding new perspectives (with guidance and best practice details) to *NESI Part 5: Technical Guidance* and *Part 6: Contracting Guidance for Acquisition*.

Part 1: Overview

- Converted v2.1 text file to a set of 19 NESI-X perspectives.

- Completely revised content of v2.1 Section 4.4 Service-Oriented Architecture in new perspective (P1304, same title).

Part 2: ASD(NII) Checklist Guidance

- Converted v2.1 text file to a set of NESI-X perspectives (with guidance and best practice details).

- Changed the title from Part 2: ASD(NII) Checklist Guidance to Part 2: Traceability to reflect the expansion from original Part 2 content to include Air Force Open Technology Development and Naval Open Architecture (and potentially other traceability in future versions).

- Removed the traceability matrices in v2.1 Section 9 and linked new perspectives (based on v2.1 text) to current and new guidance and best practices

- Moved the Relationship with the JCIDS Process perspective from Part 6 to Part 2.

Part 3: Migration Guidance

- Minimal editing changes since v2.1.

Part 4: Node Guidance

- Minimal editing changes since v2.1.

Part 5: Technical Guidance

- Added new Mobile Code perspective with five new guidance and one new best practice statements.

- Added eight new Secure Coding and Implementation Practices perspectives linked to existing guidance and best practice statements and six new best practices.

- Added new Smart Card Logon perspective with two new guidance statements.

Part 6: Contracting Guidance for Acquisition

- Added new Contracting Guidance for Intellectual Property perspective with one new guidance statement.

- Moved the Relationship with the JCIDS Process perspective from Part 6 to Part 2.

General Limitations

NESI cannot provide all of the technical guidance needed to achieve net-centricity, for the following reasons:

- Mature standards and accepted best practices do not yet exist for a number of areas that are critical to achieving desired enterprise objectives. Several hard technical questions related to net-centricity are not yet addressed or well understood given today's technologies (e.g., providing Quality of Service measures for Web services). Evolving standards and the inherent limitations in providing technical guidance about them make it likely that issues may arise concerning the compatibility across systems of different versions of the same standards as well as standards requiring specific versions of other standards. Thus, NESI guidance statements in most circumstances do not include a specific version of a standard; NESI guidance rationale normally is the area where implications of different versions of standards may be included.

- NESI does not provide a "build to" specification. The size and complexity of the enterprise combined with the rapid rate of technology evolution preclude that level of detail.

- Program-specific implementation details must be analyzed within the context of each individual program. The guidance in NESI is not intended to apply uniformly to all contexts. NESI is meant to augment, not replace, traditional systems engineering at the program level.

- NESI does not specify how to provision and deploy specific system components (e.g., services). Nor does it specify the use of specific commercial off-the-shelf (COTS) products. Acquisition managers make specific implementation choices (e.g., centralized versus distributed services and data, select specific COTS products) as appropriate within the enterprise framework as described in NESI.

- NESI does not attempt to predict the direction, progress, or capabilities of future technology.

- NESI does not address any of the processes or methodologies for developing systems (e.g., spiral development). This framework, however, is compatible with all commonly accepted methodologies and development models.

- NESI currently does not address all of the problems of real-time computing or of applications running on disconnected networks.

While NESI applies explicitly to solutions for Net-Centric Warfare, pieces of it may have applicability in a broader context.

Intended Use

NESI can help to design and implement net-centric solutions. As such, it can support a number of acquisition-related programmatic and engineering tasks:

- Prepare requirements documents

- Prepare various solicitation documents such as requests for proposals (RFPs) and statements of work (SOWs)

- Evaluate proposals

- Prepare contracts

- Prepare for general engineering reviews

- Prepare for design reviews

- Prepare for program reviews

- Perform program-level self assessments of net-centricity

- Perform enterprise-level net-centric assessments

- Prepare for program-level enterprise and application architecture reviews

In general, implementing NESI, especially in the area of assessing program net-centricity, is a Service-unique function. One potential approach is to use specific NESI guidance statements as the basis for a guided discussion between program personnel and assessment personnel. Another approach is to use NESI guidance statements to develop a program self-assessment mechanism.

While NESI can support all of these activities, it is not intended to be applied without judgment or specific program understanding.

NESI Collaboration Site

The Navy has established a collaboration site to support NESI community interaction. It is located at https://nesi.spawar.navy.mil (user registration required). Use this site for collaborative software development across distributed teams.

Detailed Perspectives

Part 1: Overview

The following Perspectives are the major components of Part1.

- NCW Introduction

- Relating DoD Net-Centric Efforts to NESI

- NESI Guidance

P1287: NCW Introduction

The purpose of **Network Centric Warfare** (**NCW**) is to increase combat effectiveness by effectively networking the warfighting enterprise.

The **ASD(NII)** *Net-Centric Checklist* [R1177] provides direction to acquisition programs for implementing NCW. NESI complements the *Net-Centrick Checklist* with more specific guidance to help obtain approval during milestone reviews. Developing systems in accordance with these principles will make the warfighter's life easier.

NCW involves much more than physical connectivity. The "network" in NCW emphasizes a network of connections between people in the information and cognitive domains. NCW stresses the shared information and situational awareness that accelerates command and synchronized efforts in the battlespace. Information systems that support NCW must exchange data seamlessly and act on a compatible understanding of the data's meaning. Specifically, they must do the following:

- Work with each other to produce coherent information, fusing many separate facts into a common picture of the battle space.

- Help users collaborate with each other to synchronize operations.

- Provide flexible information systems that can swiftly adapt to the information demands of a particular operational scenario. (This is necessary because information needs and what user collaborations must be supported are not always known in advance.)

Until now, most systems have not been built in a way that fulfills these requirements.

While the DoD is changing its usage model for information systems, various initiatives in the DoD are altering the way those information systems are produced and fielded. The public sector continually produces new technological opportunities, industry standards, and guidelines for our systems. Opportunities and challenges include the following:

- Modernize systems using new technological opportunities.

- Align with upcoming initiatives at a low cost.

- Be agile enough to reassemble capabilities to support new missions in a timely manner.

In summary, users need cohesive and flexible information systems. Ideally, they want a single, seamless system that accomplishes what they want now and changes quickly to provide what they want tomorrow. The goal of net-centricity is to deliver systems that meet these requirements.

Detailed Perspectives

- NESI Documentation Abstract

- Background

- Evolution

P1289: NESI Documentation Abstract

NESI is structured into a set of guidance products that program managers and contractors should use to achieve net-centric interoperability within their Programs of Record (PORs). The guidance is applicable during all phases of a program's lifecycle. The general guidance should be considered in all aspects of "doing business," and there are also specific examples of language that may be incorporated into program acquisition and capabilities documents (e.g., JCIDS documents, acquisition strategies and contracting artifacts). This section describes the current NESI Net-Centric Implementation Document Set, including the intended use and audience. Each audience may tailor the NESI products to their needs. Readers should use the descriptions below to choose the guidance documents most helpful for their particular program.

Part 1: Overview

Part 1 presents a high-level NESI overview to provide awareness for a variety of users including Government program managers and DoD contractors who are designing and building information systems that conform to the net-centric environment. The NESI Net-Centric Implementation documentation supports an enterprise architecture and technical implementation guidance. The architecture provides an enterprise structure and context for building mission capabilities. Use Part 1 in all phases of the acquisition process.

Part 2: Traceability

Part 2 provides a mapping of specific NESI Guidance to other, often more general, high-level DoD net-centric and interoperability efforts. Perspectives follow the structure of each high-level effort and provide a NESI interpretation of the implementation implications for program managers and developers which these other efforts direct or imply. These Perspectives, and the associated NESI Guidance and Best Practice links, provide a means of navigating NESI content based on the traceability Part 2 provides. The efforts to which Part 2 content traces may be DoD- or Service-specific; Part 2 currently traces to the **ASD(NII)** *Net-Centric Checklist*, [R1177] Air Force Open Technology Development, and Naval Open Architecture.

Part 3: Migration Guidance

Part 3 presents an approach for migrating deployed applications to greater degrees of net-centricity and interoperability. Part 3 describes the implementation of a phased software migration strategy for delivering net-centric capability while fulfilling current contractual and program maintenance obligations. It introduces an incremental, architecture-based approach to migration that identifies explicit consideration for migration to a Service-Oriented Architecture (SOA). Part 3 provides a set of flexible migration patterns organized by approximate migration starting points. It also includes a discussion of the factors to consider during migration and a detailed discussion about the process of migration.

Part 4: Node Guidance

Part 4 helps Government program managers, system engineers, and DoD contractors who develop applications and systems to conform to NESI Node guidance. This guidance specifies the criteria for building Nodes and their associated infrastructure in the net-centric environment. NESI considers a Node to be a collection of Components (i.e., systems, applications, services, and other Nodes) which results from the alignment of organizations, technologies, processes, or functions. Potential alignment attributes include management, acquisition, mission, technological, sustainment, spatial, or temporal. A Node enables the sharing of common approaches that support net-centric interoperability. Use Part 4 especially in the system acquisition phase.

Part 5: Developer Guidance

Part 5 provides developers with style guidance, detailed programming guidelines, reference software code, and open-source library references. It is intended for developers building applications, services, and components for use in the net-centric environment and is particularly useful during the system acquisition phase.

Part 6: Contracting Guidance for Acquisition

Part 6, intended for Government Program Managers and DoD contractors, briefly outlines the acquisition process and focuses on contracting guidance to support software reusability particularly during the system acquisition phase.

P1290: Background

The NESI effort developed primarily from the Air Force Command and Control Enterprise Reference Architecture (C2ERA) and the Navy Reusable Applications Integration and Development Standards (RAPIDS); however, NESI incorporates additional service-specific supportive guidance:

- Air Force Node Information Services (NIS) guidance for building loosely coupled information services using Web services technology

- Air Force XML implementation guidance for the construction and use of XML for information interchange

- Navy FORCEnet Architecture and Standards providing Navy-specific direction for migrating toward the DoD Global Information Grid (GIG)

- Naval Open Architecture

- Department of the Navy XML Developer's Guide and XML Policy

P1291: Evolution

NESI guidance will evolve along with our understanding of net-centricity. The specific details of the net-centric and enterprise capabilities referenced in these guidance documents may change. Continuous monitoring of emerging technologies, policies, and practices guides the evolution of NESI.

The NESI approach unravels functions embedded within current systems to make data and capabilities more accessible. Implicit in this approach is the potential need for retraining program managers, developers, integrators, and system administrators.

This method requires the following:

- New approaches to managing mission capabilities as services

- New monitoring tools and techniques

- New testing and deployment approaches

- New hardware and acquisition planning

- New user support functions

Recognizing the breadth and depth of this change (which represents a general rethinking of system design) is fundamental to the task of evaluating current DoD organization. The outcome of the process will be alignment with the operational shift from TPED (Task, Process, Exploit, Disseminate) toward TPPU (Task, Post, Process, Use).

P1292: Relating DoD Net-Centric Efforts to NESI

The following Perspectives describe how NESI relates to various DoD net-centric efforts.

- ASD(NII) Net-Centric Attributes

- Net-Centric Operations and Warfare Reference Model (NCOW RM)

- GIG Architecture

    - Key Interface Profiles (KIPs)

    - GES and NCES

- DoD Net-Centric Data Strategy (NCDS)

P1293: ASD(NII) Net-Centric Attributes

The Office of the Assistant Secretary of Defense for Networks and Information Infrastructure/Department of Defense Chief Information Officer, **ASD(NII)/DoD CIO**, has published the **Net-Centric Attributes List** [R1180] , with technical attributes that net-centric applications should exhibit, and the **Net-Centric Checklist** [R1177] to aid in assessing the net-centric nature of programs, projects or initiatives. The attributes list and checklist serve as the framework for NESI guidance. P1239 **ASD(NII) Net-Centric Guidance** in Part 2 maps each guidance statement to these attributes through a set of enterprise technology objectives, as described below.

Attribute	Description
Internet and World Wide Web Like	Adapting Internet and World Wide Web constructs and standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption)
Secure and Available Information Transport	Encrypted initially for core transport backbone; goal is edge to edge; hardened against denial of service
Information/Data Protection and Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling and provides provisions for assuring authenticity, integrity, and non-repudiation
Post in Parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g., raw, analyzed, archived)
Smart Pull (vice Smart Push)	Users can find and directly, subscribe or use value added services (e.g., discovery); User Defined Operational Picture vice Common Operational Picture
Information/Data Centric	Data separate from applications and services; minimize the need for special or proprietary software
Shared Applications and Services	Users can pull multiple applications to access the same data or choose the same applications when they need to collaborate; applications on "desktop" or as a service
Trusted and Tailored Access	Access to the information transport, info/data, applications and services linked to user's role, identity and technical capability
Ouality of Service	Tailored for information form: voice, still imagery, video/ moving imagery, data, and collaboration

To help focus development and maintenance actions in support of these attributes, the NESI Project Team analyzed the ASD(NII) Net-Centric Attributes List and derived the following concrete and engineering-oriented enterprise objectives.

Technology Objective	Description	Derived from ASD(NII)Net-Centric Attributes
Capability on demand	Delivery of and/or access to capabilities (data, applications, connectivity) incrementally and as needed, on demand, controlled by user clearance. Examples: • Making available new data sources in different security domains	• Information/Data Centric • Internet Protocol (IP) and World Wide Web Like • Quality of Service • Secure and Available Information Transport

	• Downloading needed applications without disrupting current operations • Reallocating communication bandwidth to meet today's operational needs and providing those needs to another organization tomorrow	• Shared Applications and Services • Trusted and Tailored Access
Distributed operations	Enable Battle Force Commanders: • Gain immediate access to essential expertise • Leverage off-board resources and expertise • Coordinate diverse aspects of operations with timely, reliable resources (i.e., trusted, remote access to collaboration environments for planning and data exchange) • Access reliable services to coordinate synchronized operations	• Assured Sharing • Internet Protocol (IP) and World Wide Web Like • Quality of Service • Secure and Available Information Transport • Trusted and Tailored Access
Customized applications	Tailor applications on a continuing basis to meet current Rules of Engagement (ROE) and readjusted to meet tomorrow's needs. For example, users can choose between a collaborative environment that allows them to access and share full-frame images or an environment for limited bandwidth communications, depending on the current need; they can adjust geographic displays to access archives of high-resolution terrain for specific, changing areas of interest.	• Information/Data Centric • Internet Protocol (IP) and World Wide Web Like • Quality of Service • Secure and Available Information Transport • Shared Applications and Services • Trusted and Tailored Access
Multi-user access	Multiple users can simultaneously access data stores, use applications, and analyze and direct operations. Examples: • Operators can develop and play back multiple ingress/ egress scenarios to accomplish more comprehensive, faster mission planning.	• Information/Data Centric • Information/Data Protection and Surety (built-in trust) • Post in Parallel • Shared Applications and Services • Smart Pull (vice Smart Push)

	• Multiple users can update data archives without overwriting each other. • Operators can use the same situational awareness picture.	• Trusted and Tailored Access
Customized delivery	Smart push and pull of data reduces overload and provides the requested data to operators when they need it. Tailored discovery, publish, and subscribe capabilities allow operators to register for specific data and services in specific timeframes. For example, operators can request track updates every four minutes. They can also request real-time data feeds that stream onto a non-real-time display for specific data types at specific times.	• Information/Data Centric • Internet Protocol (IP) and World Wide Web Like • Post in Parallel • Quality of Service • Smart Pull (vice Smart Push)
Assured sharing	Consistent authentication over the network provides trusted accessibility to resources such as data, services, applications, people, and collaborative environments. Examples: • Operators can access their data archives from diverse locations and share specific data as needed. • Essential expertise is available collaboratively. • Access to unique applications can be provided with reduced risk. • Secure access can be permitted easily and quickly.	• Quality of Service • Secure and Available Information Transport • Trusted and Tailored Access
Incremental upgrade	Certain capabilities can be modernized without impacting other capabilities. For example, developers can upgrade the display stations and software without changing how the application is used or replacing the on-board servers. They can upgrade databases without replacing applications that access the data.	• Quality of Service • Shared Applications and Services

Data exchange	Operators can move data between applications easily and without losing data or capabilities. Data may carry security labels allowing for its exchange with partners operating at coalition or multinational releasable security levels. For example, multiple applications can access a single data archive. Users can display maps identically on any display system that has access to the underlying capabilities.	• Information/Data Centric • Information/Data Protection and Surety (built-in trust) • Post in Parallel • Shared Applications and Services • Smart Pull (vice Smart Push)

P1294: Relationship to Net-Centric Operations and Warfare Reference Model (NCOW RM)

The **Net-Centric Operations and Warfare Reference Model** [R1176] describes the DoD enterprise aspects of an objective NCOW information environment for the **Global Information Grid** (**GIG**).

- Provides a common, enterprise-level reference model for the DoD enterprise architecture, and a reference for acquisition programs to use in focusing and gaining net-centric support through the GIG

- Enables a shared perspective of enterprise information environment operations

- Helps decision-makers promote enterprise-wide unity of effort

The goal is to have a uniform, DoD-wide reference for program development and oversight. Individual and enterprise programs should use it to address all net-centric IT-related issues in a consistent, coherent, and comprehensive manner.

NESI provides the technical guidance and enterprise design patterns for building net-centric capabilities as services and components that align to the NCOW RM. Within NESI, the combination of NCES and Nodes implement the NCOW RM requirements. The NCOW RM is part of the GIG Architecture described above. Compliance with the NCOW RM is one of four elements of the Net-Ready Key Performance Parameter (NR-KPP) and is assessed within the JCIDS acquisition process. Full realization of the DoD net-centric vision obligates GIG Nodes to implement portions of the NCOW RM.

NESI provides the technical guidance and enterprise design patterns for building net-centric capabilities as services and components that align to the NCOW RM, and NESI guidance is designed to promote compliance. Following the guidance will help ensure NCOW RM compliance needed for NR-KPP assessment.

The NCOW RM is described using DoDAF architectural views. The model's operational view (OV) products are most fully described, and the systems and services view (SV) products provide a high level view of the GIG, illustrating the concept of a GIG-level enterprise service infrastructure. The model reflects other DoD strategies and guidance, such as the DoD Data Strategy and the provisioning and use of the GIG Enterprise Services (GES) and Net-Centric Enterprise Services (NCES).
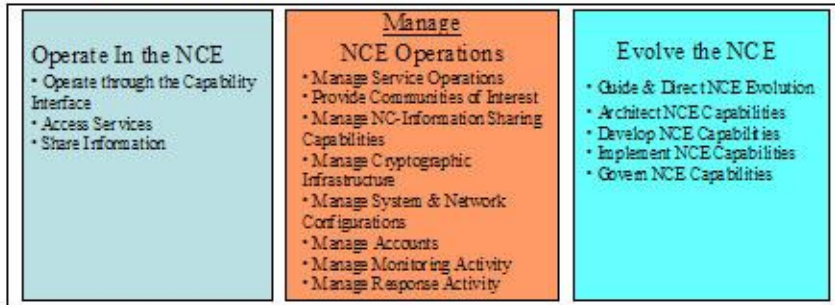
The figure below shows the three top level NCOW RM activity models from Version 1.1 (which is substantially different than the earlier Version 1.0):

- Operate in the Net-Centric Environment

- Manage Net-Centric Environment Operations

- Evolve the Net-Centric Environment

Performance of these activities is a shared obligation. DISA would typically perform some of the activities in provisioning the NCES, the Node would do some in providing and operating the local infrastructure, and the programs would do some as a matter of development and system operation. Each of these high level activities is further decomposed within the full model. The NCOW RM is viewable at https://disain.disa.mil/ncow/ncow_rm_v1_1.htm (user registration required); the home page for both the NCOW RM and GIG Architectures is https://disain.disa.mil/ncow/gigv2/index.htm (user registration required).

NCOW RM V1.1 Final
Activity Models

- *Operate in the Net-Centric Environment* - Basic Operational Model to be used by everyone.
- *Manage NCE Operations* – addresses NetOps needs.
- *Evolve the NCE* – addresses Enterprise Lifecycle Management needs (other than operations).

Operate In the NCE	Manage NCE Operations	Evolve the NCE
• Operate through the Capability Interface • Access Services • Share Information	• Manage Service Operations • Provide Communities of Interest • Manage NC-Information Sharing Capabilities • Manage Cryptographic Infrastructure • Manage System & Network Configurations • Manage Accounts • Manage Monitoring Activity • Manage Response Activity	• Guide & Direct NCE Evolution • Architect NCE Capabilities • Develop NCE Capabilities • Implement NCE Capabilities • Govern NCE Capabilities

I1210: NCOW RM v1.1 Activity Models

The JCIDS acquisition process is the enforcement mechanism for compliance with the NCOW RM, as defined in CJCSI 6212.01D [R1175] and DoD Instruction 4630.8 [R1168] . Programs that do not sufficiently address compliance risk their JCIDS **Milestone Decision Authority** (**MDA**) approval.

P1295: Relationship to GIG Architecture

The GIG architecture describes the basic, high level architecture for the GIG. It is an integrated architecture consisting of operational (OV), systems and services (SV), technical views (TV) and all-views (AV) in accordance with the DoDAF model. It provides a common lexicon and defines a basic infrastructure for the performance of information exchanges among Nodes using the GIG Enterprise Services (GES) and the Net-Centric Enterprise Services (NCES). The GIG Architecture is available at https://disain.disa.mil/ncow/gigv2/index.htm (user registration required); the home page for both the GIG architecture and **NCOW RM** is https://disain.disa.mil/ncow.html (user registration required). NESI provides implementation guidance for achieving interoperability within the GIG.

Detailed Perspectives

- Relationship to Key Interface Proviles (KIPs)

- Relationship to GES and NCES

P1297: Relationship to Key Interface Profiles (KIPs)

Key Interface Profiles (**KIPs**) specify key interfaces to the **Global Information Grid** (**GIG**). Compliance with the relevant KIPs is a **Net-Ready Key Performance Parameter** (**NR-KPP**) which is assessed at **Joint Capabilities Integration and Development System** (**JCIDS**) milestone reviews. Acquisition programs are required by CJCS Instruction 3170.01F [R1173] to comply with the relevant KIP interfaces. The NESI **Node** concept facilitates compliance with the KIPs by providing KIP-compliant infrastructure and services, rather than putting the entire burden on the individual programs. The KIPs are currently in a mixed state of definition. Originally, there were 17 Key Interface Profiles (KIPs).

1. Logical Networks to **Defense Information Systems Network** (**DISN**) Transport Backbone

2. Space to Terrestrial Interface

3. Joint Task Force (JTF) to Coalition Forces (currently limited to addressing required capabilities for the Combined Enterprise Regional Information System or CENTRIXS)

4. JTF Component to JTF Headquarters

5. Standardized Tactical Entry Point (STEP)/Teleport System

6. Joint Interconnection Service

7. DISN Service Delivery Point

8. Secure Enclave to Service Delivery Point

9. Application Servers to Database Servers

10. Client to Server

11. Application to Common Operating Environment (COE)/Common Computing Platform (CCP)

12. End System to **Public Key Infrastructure** (**PKI**)

13. Management Systems to Integrated Management Systems

14. Management Systems to Managed Systems

15. Information Dissemination Management (IDM) to Distribution Infrastructure

16. Information Services to IDM Infrastructure

17. Applications to Shared Data

The KIPs are now being reformed according to a KIP Framework (draft) shown in the following figure.

KIP Framework
(one document)

Transport
Family of KIPs
(one document)

Computing Infrastructure
Family of KIPs
(one document)

Application Enterprise Services
Family of KIPs
(one document)

- **Rules for Entire Family**
- **Individual KIPs (Appendices)**
  - **UHF SATCOM**
  - **Global Broadcast Service**
  - **Next Generation DISN**
    .
    .
    .

- **Rules for Entire Family**
- **Individual KIPs (Appendices)**
  - **DECC Equivalency**
    .
    .
    .

- **Rules for Entire Family**
- **Individual KIPs (Appendices)**
  - **Content Discovery**
  - **Service Discovery**
  - **Security**
    .
    .
    .

KIP Configuration
Management Plan
(one document)

KIP Test and
**Evaluation Strategy**
(one document)

I1212: KIP Taxonomy

NESI provides guidance that helps programs comply with the KIPs. NESI also identifies some implementation issues, such as the federation of services and disconnected operations, and provides guidance where available.

P1298: Relationship to GES and NCES

The Department of Defense (DoD) is defining services for provision and use across the entire scope of the **Global Information Grid** (**GIG**); collectively, these are the **GIG Enterprise Services** (**GES**). A subset of these, called the **Net-Centric Enterprise Services** (**NCES**), include both fundamental enabling services needed to support the DoD net-centric goals and services that are common to communities of users or are utilitarian. The fundamental services for achieving net-centric goals are called the **Core Enterprise Services** (**CES**). The CES services are at various states of definition, piloting, and rollout. The common and utilitarian services are called **Community of Interest** (**COI**) services. This document focuses on the CES services as basic enablers of interoperability between GIG Nodes.
The **Defense Information Systems Agency** (**DISA**) is managing CES development as an agent for **ASD(NII)**. Recognizing that there are complex interdependencies between elements of the CES, services development has been organized into product lines.

The NCES Pilot Participants Guide for the **NIPRNet**, developed as part of an Early Adopters effort, which describes how to participate in enterprise service pilots. For most sites, piloting would probably be done through a development, integration, and test cycle.
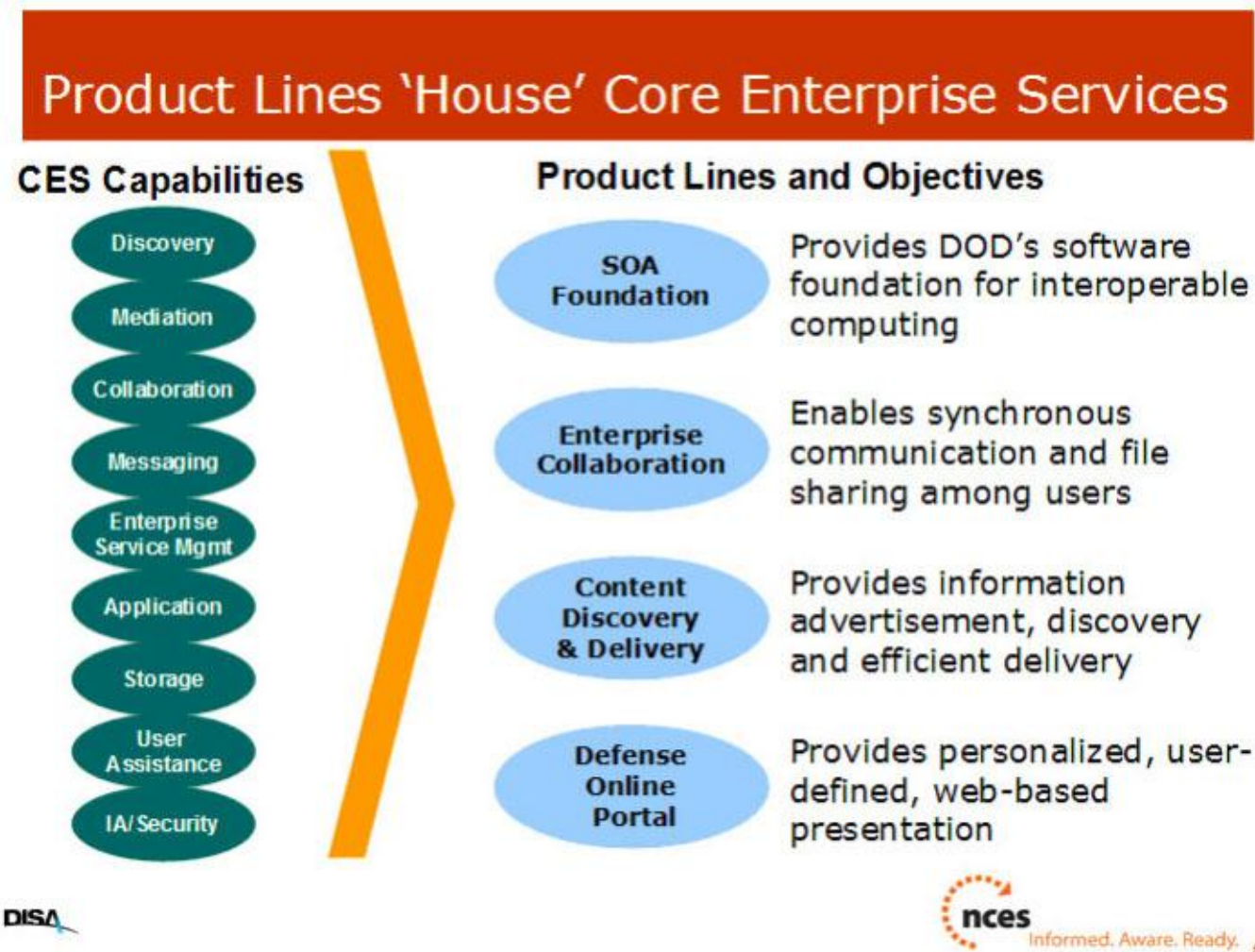
I1213: Organization of CES into Product Lines

The NCES and GES home pages are available through the Defense Knowledge Online (DKO) portal at https://www.us.army.mil/ (user registration required).

NESI provides guidance applicable to coordinating and implementing services in alignment with NCES efforts.

P1299: Relationship to the DoD Net-Centric Data Strategy

The DoD has developed a **DoD Net-Centric Data Strategy** (**NCDS**), along with associated policies and guidance. NESI contains guidance which addresses data or information engineering. Data engineering is as much a social and cultural challenge as it is a technical challenge. It is not a stand-alone activity. **Community of Interest** (**COI**) forums have the task of data engineering, and the **DoD Metadata Registry** (MDR) is the primary tool for managing data engineering across the **GIG**. MDR instances exist on the **NIPRNet**, **SIPRNet**, and **JWICS** networks.

P1300: NESI Focus Areas

Today there is no single, comprehensive technology deployment suitable for the entire DoD Enterprise. The complexity of the enterprise makes centralized implementation impractical. Its survivability requires independent, redundant, loosely-coupled entities.

The core technical concept of net-centricity is a completely secure network that is accessible worldwide. The network must deliver messages in a timely manner, such that the application or human who receives them can make decisions appropriately. The messages are either for services ("do something") or for information ("tell me what I need to know").

The net-centric vision needs to be concrete and explicit so that systems can implement it. Both legacy and new applications need simple, transparent, robust methods to acquire and share information across traditional system, service, and community boundaries.

NESI contributes to this vision by providing implementation guidance for building solutions to satisfy this vision.

Detailed Perspectives

- Information Interoperability

- Communities of Interest

- NESI Elements

- Service-Oriented Architecture

- Enterprise Services

- Nodes

P1301: Information Interoperability

Net-centricity requires applications to share information with each other. To do this, applications must be able to exchange data and to agree on its meaning.

The first part requires access to data. That is, one application must be able to obtain data provided by another. NESI facilitates this by providing a least-common-denominator data access mechanism that all applications can use. This removes arbitrary implementation barriers to data exchange. NESI also includes guidance for adding customizability to applications, including "on-the-fly" reconfiguration.

The second part requires a *semantic match* between users and developers. That is, users and developers must be able to determine whether the data they receive is suitable for their purpose, and they must be able to cope with any *representation mismatch*. For example, if the source application provides volume measurements in gallons, but the receiving application requires liters, then a translation function must be applied. NESI does not directly address semantics at this time. The necessary shared understanding will be supported by common vocabularies developed by **Communities of Interest**.

P1302: Communities of Interest

NESI provides significant guidance for building systems that support **Communities of Interest** (COIs). A **COI** is a collaborative group of users who exchange information for their shared goals, interests, missions, or business processes. The success of this exchange depends on a shared vocabulary. Within NESI, COIs have the following properties:

- A COI is a group of people who share a common vocabulary. There is typically a deliberate effort to produce this community vocabulary.

- A COI may be institutional, expedient, functional, or cross-domain.

- A COI may be a subset of another COI.

- A COI always encompasses more than one system or Node. A system is a source of data and/or capability, and often participates in more than one COI.

- A COI typically encompasses more than one organization.

P1303: NESI Elements

NESI organizes the enterprise into three elements:

- *Enterprise Services* provide enterprise-wide capabilities to link **Nodes**, **services**, **applications**, and **components**.

- *Nodes* provide local infrastructure to support local services, applications, and components.

- *Services*, *Applications*, and *Components* integrate with the Node infrastructure to provide mission capabilities the warfighters need.

NESI supports an N-tier architecture that includes presentation, middle, and data tiers. NESI relies upon the **Net-Centric Enterprise Services** (**NCES**) program (see P1305). The combination of NESI and NCES yields an open-standards architecture that allows the **enterprise** to encapsulate the elements of existing or new systems. The elements plug together seamlessly and can be upgraded and expanded more easily.

Mature standards and accepted best practices do not yet exist for a number of areas that are critical to achieving desired enterprise objectives. Several hard technical questions related to net-centricity are not yet addressed or well understood given today's technologies (e.g., providing **Quality of Service** measures for **Web services**). Evolving standards and the inherent limitations in providing technical guidance about them make it likely that issues may arise concerning the compatibility across systems of different versions of the same standards as well as standards requiring specific versions of other standards. Thus, NESI guidance statements in most cases do not include a specific version of a standard; NESI guidance rationale normally is the area where implications of different versions of standards may be included.

The NCES architecture does not currently provide detailed guidance for developing systems or applications to support COIs. NESI complements NCES by expanding the guidance for COIs and for the infrastructure required to build mission applications that integrate into COIs and the enterprise.

The DoD Enterprise includes software components delivered by different organizations on different schedules. All components, however, are organized around the architecture shown in the figure below which shows the types of components that coexist in the enterprise and support each other.
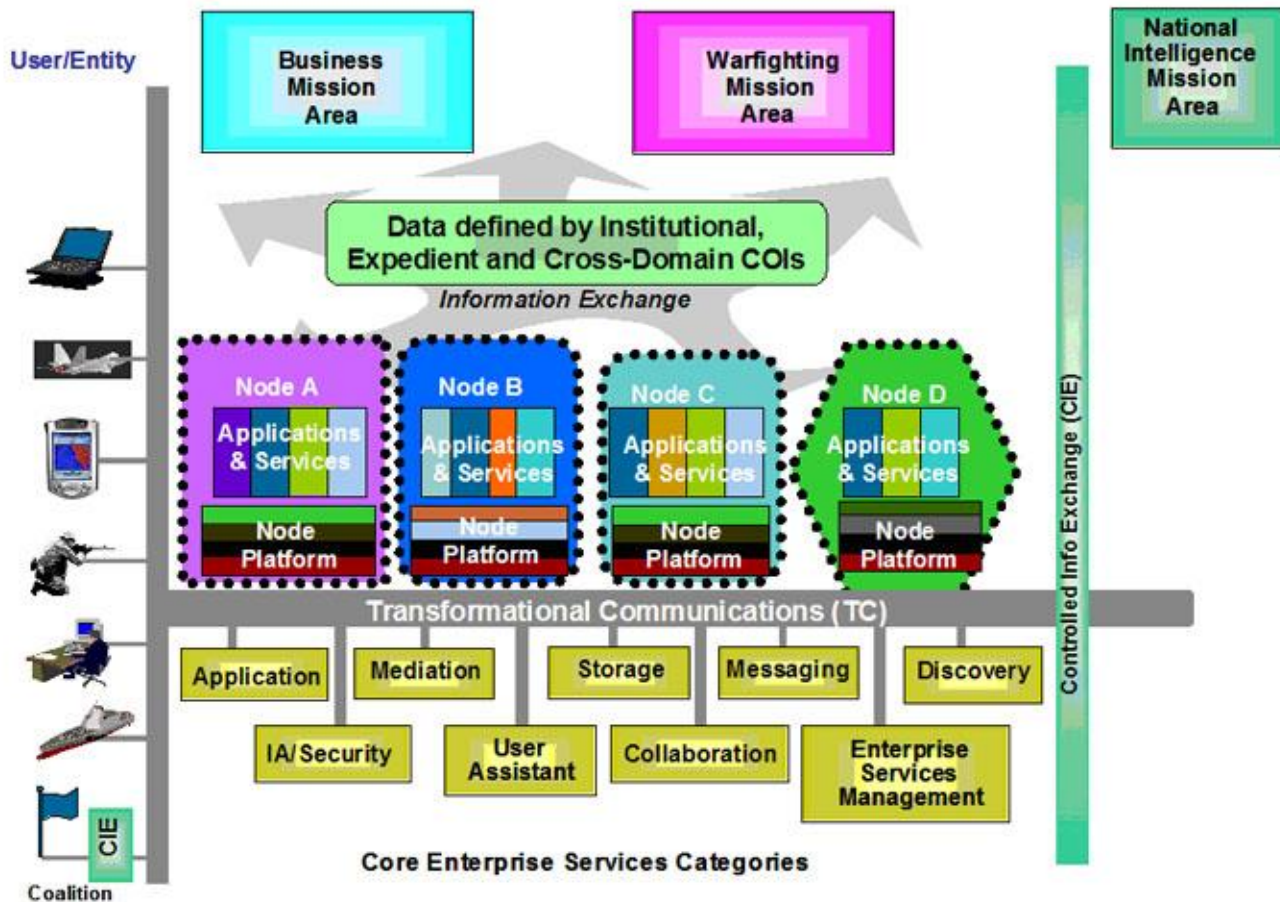
I1215: DoD Net-Centric Enterprise

At the top of the figure are three basic DoD domains: business operations, warfighting and intelligence. COIs that share data form within and across these domains.

The Node provides the infrastructure that supports COIs. The figure shows several Node instances which communicate using the **GIG**. Nodes provide or make use of core services (shown at the bottom of the figure) to support inter-Node activities such as messaging.

NCES services will not meet all internal needs of Nodes and COIs. The local Node infrastructure provides services for applications and users within the COI and Node.

P1304: Service-Oriented Architecture

There are many definitions of a **Service-Oriented Architecture** (**SOA**) from a variety of organizations, committees, and individuals such as the following:

- DoD ***Net-Centric Warfare and Operations Reference Model (NCOW RM)*** [R1176]

- Organization for the Advancement of Structured Information Standards (OASIS) ***Reference Model for Service Oriented Architecture 1.0*** [R1308]

- The Open Group ***Service-Oriented Architecture (SOA)*** [R1309]

- ***SOA Practitioners' Guide Part 2 SOA Reference Architecture*** [R1310]

This perspective does not provide a new definition of what a Service-Oriented Architecture is but rather explains SOA as an **architectural style** with specific characteristics. An architecture implemented in a particular architectural style often does not express all of the style characteristics. Consequently, as with most styles, there is no single expression of the SOA style. Also, a "SOA" cannot be acquired per se; rather, one acquires or builds solutions that fit the SOA style.

> ***Note:*** *This is analogous to other styles such as Impressionistic or Art Nuevo. No one buys an "Impressionistic" or an "Art Nuevo" but rather a painting that is of the Impressionistic style or a house built in the Art Nuevo style.*

NESI describes SOA as an architectural style used to design, develop, and deploy information technology (IT) systems based on decomposing functionality into **services** with well-defined interfaces. In SOA a set of modular, decentralized, composeable, loosely coupled services provide functionality to consumers. SOA allows service provider and consumer implementations to evolve independently.

In this perspective, as well as throughout NESI, the terms "SOA" and "SOA Architectural Style" are interchangeable, with the exception of when "SOA" is an adjective in other contexts (e.g., "SOA infrastructure").

The cornerstone of SOA is the concept of a service as an autonomous encapsulation of some business or mission functionality. The service concept includes the notion of service providers and service consumers interacting via well-defined interfaces. An implementation of a service generally has the following characteristics:

- Logical representation of a repeatable business or mission functionality

- Loosely coupled, independent, autonomous, manageable, shareable implementation as a software agent

- Support of one-to-one as well as many-to-many relationship between service providers and service consumers

- Contract for predictable behavior between a service provider and a service consumer

    - Standard description of capability (e.g., Service Definition Framework or SDF)

    - Well-defined interfaces

        - Based on open standards

        - Programming language neutrality

        - Isolation from internal implementation of the service

    - Service Level Agreements (SLAs)

- Location transparency

- Invocable over the network

- Net-centric, discoverable location

- Loose coupling-based composeability (involves no changes to services, compilations or linking)

  - Ability to assemble services from other services

  - Functionality of a service composeable from multiple functionalities without affecting the existing ones (e.g., combining multiple Web Services specifications)

There is a key distinction between what is the "service" and the technological mechanisms that implement it. SOAP-based Web services, publishing services, RESTful services, etc., are all technological mechanisms which implement services and support their interactions with an environment. The service concept can capture almost any business or mission functionality and implement it using any number of technological mechanisms.

Services with a common scope are woven into an architecture implemented in SOA style where they are composed around mission threads or business processes. The scope may be at any operational (business) level and may cross traditional management boundaries.

The computing infrastructure that supports and enables the implementation of services is often called "SOA Infrastructure." Often, the functionality provided by the infrastructure itself is expressed in terms of services, which should not be confused with the "application services" that use the infrastructure. The notions of "SOA Infrastructure" and "Service-Oriented Infrastructure" are distinct from the more general concept of SOA and SOA services.

P1305: Enterprise Services

Enterprise services and Nodes provide infrastructure capabilities that underlie the **SOA** paradigm.
NCES defines a set of **core enterprise services**. NCES services are the set of net-centric utilities that the **DoD**
and **Defense Information Systems Agency** (**DISA**) defined to enable secure, reliable, timely, and interoperable
information exchange.

The **GIG** architecture allows for additional domain and mission-related services, called **COI services**, which extend the
enterprise beyond NCES. Services provided by Nodes will generally be developed as COI services.

NESI guidance is primarily intended for developers of systems that provide and use COI services and use NCES services.

Net-Centric Enterprise Services

The **Net-Centric Core Enterprise Services** (NCES; https://ges.dod.mil/; user registration required) program will
provide enterprise-level **Information Technology** (**IT**) services and infrastructure components for the DoD GIG.
The net-centric enterprise relies on the NCES infrastructure. NCES in turn relies on GIG transport services such as
the **Defense Information System Network** (**DISN**) and tactical communications systems. While NCES relies upon
the GIG transport services, visibility into transport details is not an inherent component of NCES.

Many of the NCES services referenced in NESI guidance are evolving. The implementer should use these services
where available. Where they are not yet available, the developer should provide an application-specific, Nodal,
or COI implementation based on the NCES interface definition. The developer should design the implementation
based on best commercial practice so that it is straightforward to replace it with the NCES implementation of the
service, when that is deployed.

P1306: Nodes

This section summarizes the key principles and characteristics of **Nodes** in the NESI context. See *Part 4: Node Guidance* [P1130] for details on Nodes.

A Node is a collection of **Components** (i.e., **systems**, **applications**, **services**, and other Nodes) which results from the alignment of organizations, technologies, process, or functions. Potential alignment attributes include management, acquisition, mission, technological, sustainment, spatial, or temporal. A Node enables the sharing of common approaches that support net-centric interoperability. As a concept, Nodes may not be defined in terms of a concrete set of Components or size.

Nodes represent a departure from the past "stovepipe" acquisition and development of single systems with tightly integrated infrastructure and mission function. Factors such as physical environments and employment concepts directly influence a Node's scope, and boundaries can vary widely. Nodes typically contain systems, applications, and components that have similar missions and locality. However, Nodes are not limited to supporting similar missions and can be geographically distributed or aligned across other parameters.

Common needs as well as external interoperability requirements drive the definition of a Node's infrastructure, services, components, and applications. *Part 4: Node Guidance* focuses on identifying a set of guidance for achieving integration and interoperability of Nodes within the GIG; additional Part 4 guidance is meant for those in a position to influence decisions regarding infrastructure and services provided by the Node for shared use by the systems within the Node. With respect to the GIG, the principal question addressed is, "What and how should a Node implement the shared infrastructure needed to achieve the DoD vision of broad integration and interoperability across the GIG, on behalf of systems within the Node, and in accordance with DoD policy and direction?" Part 4 focuses on guidance for achieving integration and interoperability in this context without excluding additional capabilities that may be needed to satisfy specific operational needs.

The guidance is applicable to information systems, such as those for command and control or intelligence. Nodes can include components such as Web servers, portal servers, application servers, and database servers. Nodes share information with other Nodes connected to the enterprise network according to **COI**-defined standards for information content, structure, and format implemented by the services, applications, and components within the Node. Some Nodes may require continued (though probably degraded) operation even when disconnected from the GIG and must therefore provide local services while maintaining interoperability with the enterprise.

The figure below depicts a notional DoD enterprise based on Nodes.
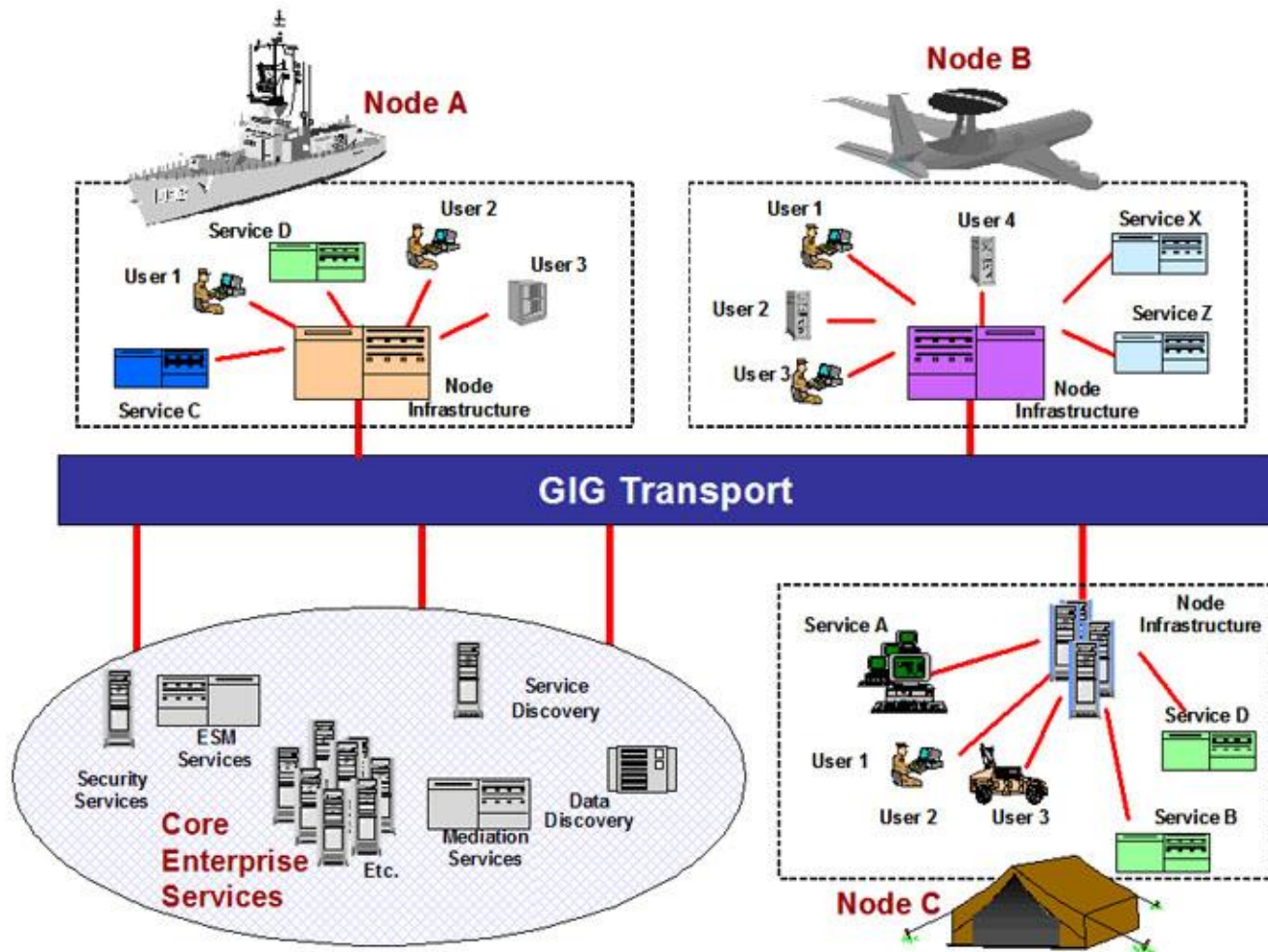
I1217: Nodes in the Enterprise

The net-centric enterprise comprises a set of Nodes, where each Node comprises a set of mission functions and services implemented on a common infrastructure. The enterprise can be managed as a collection of Nodes without concern for the intra-Node implementation details.

Nodes optimize their infrastructure and services to support their missions. The enterprise is optimized to provide continuity, consistency, interoperability, and persistence across the enterprise.

Glossary

Application		Provides the resources necessary to provision, operate and maintain **Net-Centric Enterprise Services** (NCES) capabilities.
Architectural Style		An architectural style is the combination of distinctive features in which **architecture** is performed or expressed. (Source: http://www.opengroup.org/projects/soa/doc.tpl?gdid=10632)
Architecture		(1) The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. (2) A high-level design that provides decisions about the problem(s) that the product will solve, component descriptions, relationships between components, and dynamic operation description. (3) A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. Also, the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution. The organizational structure of a system or component, their relationships, and the principles and guidelines governing their design and evolution over time. (Source: IEEE Std 610.12)
Assistant Secretary of Defense for Networks and Information Integration	ASD (NII)	(Source: http://www.dod.mil/nii/)
Community of Interest	COI	A COI is a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes nd therefore must have shared vocabulary for the information it exchanges. (Source: DoDD 8320.02, 2 December 2004, *Data Sharing in a Net-Centric Department of Defense*)
Community of Interest Service		A service that may be offered to the enterprise, but is owned and operated by a **Community of Interest** to provide or support a well-defined set of mission functions and associated information.
Component		One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components. Note the terms *module*, *component*, and *unit* are often used interchangeably or defined to be sub-elements of one another in different ways depending on the context. The relationship of these terms is not yet standardized. (Source: IEEE Std 610.12-1990) **Note:** See **system component** and **software component**.
Core Enterprise Services	CES	Ubiquitous, common solution **services** that provide capabilities essential to the operation of the enterprise.

		Generic information services that apply to any **COI**, provide the basic ability to search the **enterprise** for desired information, and then establish a connection to the desired service. (Source: http://www.defenselink.mil/nii/org/cio/doc/GIG_ES_Core_Enterprise_Services_Strategy_V1-1a.pdf)
Defense Information System Network	DISN	The Defense Information System Network (DISN) has been the Department of Defense's enterprise network for providing data, video and voice services for more than 40 years. (Source: http://www.disa.mil/main/support/dss.html)
Defense Information Systems Agency	DISA	Combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. (Source: http://www.disa.mil/main/about/missman.html)
Department of Defense	DoD	A civilian Cabinet organization of the United States government. The Department of Defense controls the U.S. military and is headquartered at The Pentagon. It is headed by the Secretary of Defense. (Source: http://en.wikipedia.org/wiki/United_States_Department_of_Defense)

DoD Metadata Registry		As part of the overall **DoD Net-Centric Data Strategy**, the DoD CIO established the DoD Metadata Registry (http://metadata.dod.mil) and a related metadata registration process for the collection, storage and dissemination of structural metadata information resources (schemas, data elements, attributes, document type definitions, style-sheets, data structures, etc.). This Web-based repository is designed to also act as a clearinghouse through which industry and government coordination on metadata technology and related metadata issues can be advanced. As OASD's Executive Agent, **DISA** maintains and operates the *DoD Metadata Registry and Clearinghouse* under the direction and oversight of **OASD(NII)**. (Source: DoD Metadata Registry v6.0 Web site, https://metadata.dod.mil/mdr/about.htm)
DoD Net-Centric Data Strategy		This Strategy lays the foundation for realizing the benefits of net-centricity by identifying data goals and approaches for achieving those goals. To realize the vision for net-centric data, two primary objectives must be emphasized: (1) increasing the data that is available to communities or the Enterprise and (2) ensuring that data is usable by both anticipated and unanticipated users and applications. (Source: *Department of Defense Net-Centric Data Strategy*, DoD CIO, 9 May 2003, http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf)
Enterprise		An organization considered as an entity or system that includes interdependent resources (e.g., people, organizations, and technology) that must coordinate functions and share information in support of a common mission or a set of related missions. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. (Source: http://www.webopedia.com/TERM/e/enterprise.html)
eXtensible Markup Language	XML	A markup language defines tags (markup) to identify the content, data, and text in XML documents. It differs from **HTML**, the markup language most often used to present information on the Internet. HTML has fixed tags that deal mainly with style or presentation. An XML document must undergo a transformation into a language with style tags under the control of a style sheet before it can be presented by a browser or other presentation mechanism. Two types of style sheets used with XML are CSS and XSL. Typically, XML is transformed into HTML for presentation. Although tags can be defined as needed in the generation of an XML document, you can use a document type definition (DTD) to define the elements allowed in a particular type of document. A document can be compared by using the rules in the DTD to determine its validity and to locate particular elements in the document. A Web services application's J2EE deployment descriptors are expressed in XML with schemas defining allowed elements. Programs for processing XML documents use SAX or DOM APIs. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)

GIG Enterprise Service		A service that provides capabilities for use in the DoD enterprise. GIG Enterprise Services are the combination of Core Enterprise Services and Community of Interest Services. Also referred to as Global Enterprise Services.
Global Command and Control System	GCCS	GCCS-J is the DOD joint C2 system of record for achieving full spectrum dominance. It enhances information superiority and supports the operational concepts of full-dimensional protection and precision engagement. GCCS-J is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture of the battlespace necessary to conduct joint and multinational operations. It fuses select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information. GCCS-J offers vital connectivity to the systems the joint warfighter uses to plan, execute, and manage military operations. GCCS-J is a Command, Control, Communications, Computer, and Intelligence (C4I) system, consisting of hardware, software, procedures, standards, and interfaces that provide a robust, seamless C2 capability. The system uses the Defense Information Systems Network (DISN) and must work over tactical communication systems to ensure connectivity with deployed forces in the tactical environment. (Source: http://www.disa.mil/gccs-j/)
Global Information Grid	GIG	Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.
Hypertext Markup Language	HTML	A markup language for hypertext documents on the Internet. HTML supports embedding images, sounds, video streams, form fields, references to other objects with URLs, and basic text formatting. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Hypertext Transfer Protocol	HTTP	The Internet protocol used to retrieve hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. (Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Information Technology	IT	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition,

		storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract. (Source: CJCSI 6212.01D, 8 March 2006, Glossary page GL-11)
Java 2 Platform, Enterprise Edition	J2EE	The J2EE environment is the standard for developing component-based multi-tier enterprise applications. The J2EE platform consists of a set of services, application programming interfaces (APIs), and protocols that provide the functionality for developing multitiered, Web-based applications. Features include Web services support and development tools. Sun Microsystems has simplified the name of the Java platform for the enterprise; the "2" is dropped from the name, as well as the dot number so the next version of the Java platform for the enterprise is **Java Platform, Enterprise Edition** 5 or Java EE 5.(Source: http://java.sun.com/j2ee/1.4/docs/glossary.html)
Java Platform, Enterprise Edition	Java EE	Java Platform, Enterprise Edition (Java EE) is the industry standard for developing portable, robust, scalable and secure server-side Java applications. Building on the solid foundation of the Java Platform, Standard Edition (Java SE), Java EE provides Web services, component model, management, and communications APIs that make it the industry standard for implementing enterprise-class service-oriented architecture (SOA) and next-generation Web applications. Sun Microsystems has simplified the name of the Java platform for the enterprise. Formerly, the platform was known as Java 2 Platform, Enterprise Edition (**J2EE**), and specific versions had "dot numbers" such as J2EE 1.4. The "2" is dropped from the name, as well as the dot number so the next version of the Java platform for the enterprise is Java Platform, Enterprise Edition 5 or Java EE 5. (Source: http://java.sun.com/javaee/)
Joint Capabilities Integration and Development System	JCIDS	Establishes procedures to support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying, assessing and prioritizing joint military capability. (Source: CJCSI 3170.01E, 11 May 2005, *Joint Capabilities Integration and Development System*)
Joint Worldwide Intelligence Communications System	JWICS	The sensitive, compartmented information portion of the **Defense Information Systems Network**. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. (Source: http://www.dtic.mil/doctrine/jel/doddict/data/j/02972.html)
Key Interface Profile	KIP	An operational functionality, systems functionality and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, interface control specifications, Technical View with SV-TV

		Bridge, and referenced procedures for KIP compliance. The key interface profile is the technical specification that governs access to the **GIG**. (Source: CJCSI 6212.01D, 8 March 2006, Glossary page GL-14)
Milestone Decision Authority	MDA	The individual designated, in accordance with criteria established by the Under Secretary of Defense for Acquisition, Technology and Logistics, the Assistant Secretary of Defense (Networks and Information Integration) (for Automated Information System acquisition programs) or by the Under Secretary of the Air Force (as the DOD Space MDA) to approve entry of an acquisition program into the next phase. (Source: CJCSI 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005)
Net-Centric Enterprise Services	NCES	The NCES program provides enterprise-level Information Technology (IT) services and infrastructure components, also called Core Enterprise Services, for the Department of Defense (DoD) Global Information Grid (GIG).
Net-Centric Enterprise Solutions for Interoperability	NESI	A cross service effort between the U.S. Navy Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I), the U.S. Air Force Electronic Systems Center (ESC) and the Defense Information Systems Agency (DISA). NESI provides a reference architecture, implementation guidance, and a set of reusable software components. These facilitate the design, development, maintenance, evolution, and use of information systems for the Net-Centric Operations and Warfare (NCOW) environment.
Net-Centric Operations and Warfare Reference Model	NCOW RM	The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic userinterface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, **Community of Interest (COI) services**, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the **Global Information Grid** (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; **DoD** business operations; and Department-wide enterprise management operations. The NCOW RM is a key compliance mechanism for evaluating DoD information technology capabilities and the **Net-Ready Key Performance Parameter**. (Source: CJCSI 6212.01D, 8 March 2006, Glossary pages GL-17 and GL-18)
Net-Ready Key Performance Parameter	NR-KPP	The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely,

		accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements: • Compliance with the **NCOW RM**. • Compliance with applicable **GIG KIPs**. • Verification of compliance with DoD information assurance requirements. • Supporting integrated architecture products required to assess information exchange and use for a given capability. (Source: DoD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004, [R1168] Enclosure 2 Section E2.1.51)
Network Centric Warfare	NCW	NCW is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of selfsynchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace. (Source: *Network Centric Warfare: Developing and Leveraging Information Superiority*. David S. Alberts, John J. Garstka and Frederick P. Stien. DoD Command and Control Research Program Publication Series, available at http://www.dodccrp.org/files/Alberts_NCW.pdf)
Node		In general network usage, a node is a processing location such as a computer or some other device. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address. (Source: http://www.webopedia.com/TERM/n/node.html) A NESI Node is a collection of integrated components (i.e., systems, applications, services and other Nodes) that are bound together spatially and/or temporally to meet the needs of a particular mission. It is conceptual in nature and can not be defined in terms of a concrete set of components or size. The membership of a component within a particular Node is not exclusive and a Component can be part of multiple Nodes.
Public Key Infrastructure	PKI	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (Source: CNSS Instruction No. 4009, Revised May 2003, *National Information Assurance (IA) Glossary*)
Quality of Service	QoS	Data timeliness, accuracy, completeness, integrity, and ease of use. Refers to the probability of the network meeting a given traffic contract. In many cases is used informally to

		refer to the probability of a packet passing between two points in the network. (Source: http://en.wikipedia.org/wiki/Quality_of_service) -OR- A defined level of performance that adapts to the environment in which it is operating. QoS may be requested by the user of the information. The level of QoS provided is based on the request, the available capabilities of the provider, and the priority of the user.
Secret Internet Protocol Router Network	SIPRNet	DoD's largest interoperable command and control data network, supporting the **Global Command and Control System** (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56 kbps to 155 Mbps for the **Unclassified but Sensitive Internet Protocol Router Network** (NIPRNet), and up to 45 Mbps for the SIPRNet. Remote dial-up services are also available, ranging from 19.2 kbps on SIPRNet to 56 kbps on NIPRNet. (Source: http://www.disa.mil/main/prodsol/data.html)
Service		A service is an autonomous encapsulation of some business or mission functionality. The service concept includes the notion of service providers and service consumers interacting via well-defined reusable interfaces. *Note: See P1304: **Service-Oriented Architecture** in Part 1 for additional information concerning services including implementation characteristics.*
Service-Oriented Architecture	SOA	NESI describes SOA as an architectural style used to design, develop, and deploy information technology (IT) systems based on decomposing functionality into services with well-defined interfaces. *Note: See P1304: **Service-Oriented Architecture** in Part 1 for additional information.*
Single Integrated Air Picture	SIAP	The SIAP is the product of fused, common, continuous, unambiguous tracks of all airborne objects in the surveillance area. Each object within the SIAP has one, and only one, track number and set of associated characteristics. The SIAP is developed from near-real time and real time data, and is scalable and filterable to support situation awareness, battle management, and target engagements. JTAMDO Battle Management Concept.

SOAP		SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics. (Source: SOAP Version 1.2 Second Edition, http://www.w3.org/TR/soap12-part1/#intro) **Note:** *The World Wide Web Consortium (W3C) changed the name of this protocol from **Simple Object Access Protocol 1.1 (SOAP)** to **SOAP Version 1.2** in the current version.*
Software Component		A software component is a software system element offering a predefined service and able to communicate with other components. It is a unit of independent deployment and versioning, encapsulated, multiple-use, non-context-specific and composeable with other components. Source: http://en.wikipedia.org/wiki/Software_component#Software_component
System		Two or more interrelated pieces of equipment (or sets) arranged in a package to perform an operational function or to satisfy a requirement. (Source: *Defense Acquisition Glossary of Terms*, Jan 2001)
System Component		A basic part of a system. System components may be personnel, hardware, software, facilities, data, material, services, and/or techniques that satisfy one or more requirements in the lowest levels of the functional architecture. System components may be subsystems and/or configuration items. **Note:** See **component**.
Unclassified but Sensitive Internet Protocol Router Network	NIPRNet	NIPRNet provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. Direct connection data rates range from 56Kbps to 622Mbps. Remote dial-up services are available up to 56Kbps. (Source: http://www.disa.mil/main/prodsol/data.html)
Web Service		A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically **WSDL**). Other systems interact with the Web service in a manner prescribed by its description using **SOAP** messages, typically conveyed using **HTTP** with an **XML** serialization in conjunction with other Web-related standards. (Source: http://www.w3.org/TR/ws-gloss/)
Web Services Description Language	WSDL	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The

		operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. (Source: W3C Note on WSDL 1.1 of 15 March 2001 http://www.w3.org/TR/wsdl)

References

R1164	DoD Directive 5000.1, *The Defense Acquisition System*, 12 May 2003 (certified current as of 24 November 2003); http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.
R1165	DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, 12 May 2003; http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf.
R1166	DoD Directive 8100.1, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002 (certified current as of 21 November 2003); http://www.dtic.mil/whs/directives/corres/pdf/810001p.pdf.
R1167	DoD Directive 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 05 May 2004 (certified current as of 23 April 2007); http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf.
R1168	DoD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004; http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf.
R1170	*DoD Global Information Grid (GIG) Architecture*, Version 2.0, August 2003.
R1171	*DoD Architecture Framework (DoDAF)*, Version 1.5, 23 April 2007; https://dars1.army.mil/IER/index.jsp
R1172	*DoD Net-Centric Data Strategy*, DoD Chief Information Officer, 9 May 2003, http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf.
R1173	CJCSI 3170.01F, *Joint Capabilities Integration and Development System*, 01 May 2007; http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01new.pdf.
R1174	CJCSM 3170.01C, *Operation of the Joint Capabilities Integration and Development System*, 01 May 2007; http://www.dtic.mil/cjcs_directives/cdata/unlimit/m317001.pdf.
R1175	CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems*, 8 March 2006; http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf.
R1176	*Net-Centric Operations and Warfare Reference Model (NCOW RM)*, v1.1, 17 November 2005.
R1177	*Net-Centric Checklist*, V2.1.3, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004; http://www.defenselink.mil/cio-nii/docs/NetCentric_Checklist_v2-1-3_.pdf.
R1178	*A Modular Open Systems Approach (MOSA) to Acquisition*, Version 2.0, September 2004; http://www.acq.osd.mil/osjtf/mosapart.html.
R1179	*DoD IT Standards Registry* (*DISR*); http://disronline.disa.mil.
R1180	*Net-Centric Attributes List*, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 2 February 2007; http://www.defenselink.mil/cio-nii/docs/NetCentricAttributesOfficial.pdf .

R1181	*Global Information Grid (GIG) Key Interface Profiles (KIPs) Framework* (DRAFT), Version 0.95, 7 October 2005.
R1232	DoD Directive 5230.9, **Clearance of DoD Information for Public Release**, 09 April 1996
R1308	OASIS **Reference Model for Service Oriented Architecture 1.0**, Committee Specification 1, 2 August 2006; http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf
R1309	The Open Group, **Service-Oriented Architecture**; http://www.opengroup.org/projects/soa/doc.tpl?gdid=10632
R1310	The SOA Alliance, **SOA Practitioners' Guide Part 2 SOA Reference Architecture**, 15 September 2006; http://soablueprint.com/yahoo_site_admin/assets/docs/SOAPGPart2.290211443.pdf